DISA JIEO Standards Analysis **13 MAY 99**

Key Usage Extension: nonRepudiation bit

References: X.509 sections: 11.2, 12.2.2.3, B.3
RFC 2459 sections: 2, 4.2.1.3, 4.2.1.13, 7.3.1, 7.3.3
FPKI Profile section: 1.2.3, 3.2.2.1.1
DII PKI Functional Specification sections: 2.4,
3.2.2.1.3, Appendix A

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Is it a matter for the security policy and responsibility of the certification authority (CA) to keep old certificates for a period if a non-repudiation of data service is provided?		
If a non-repudiation service is dependent on keys provided by the CA, does the service ensure that all relevant CA keys (revoked or expired) and the timestamped revocation lists are archived and certified by a current authority?		
If the certificate issuer sets the nonRepudiation (NR) bit, does it mark the key usage (KU) extension critical?		
Does the certificate issuer set the NR bit in Identity Certificates?		
Does the certificate issuer set the NR bit in EE Standard Digital Signature and SSL Client Certificates?		
Does the certificate user interpret the setting of KU bit 1 as NR?		
Does the certificate user review the CA's certificate policy before relying on the non-repudiation services associated with the public key in a particular certificate?		
When NR is set, is the certified public key used to verify a digital signature providing non-repudiation service that protects against the signing entity falsely denying some action, excluding certificate or		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
When only the NR bit is set, and the extension is flagged critical, is the verified digital signature not used to provide authentication and integrity services?		
Is the certificate-using system able to process a certificate with both the NR bit set and the Extended key usage field present containing the E-mail protection and/or time stamping OID?		
Are the KU keyAgreement, keyCertSign, cRLSign, encipherOnly, and decipherOnly bits not set when the NR bit is set in an EE certificate conveying a RSA public key?		
Are the KU keyAgreement, encipherOnly, and decipherOnly bits not set when the NR bit is set in a CA certificate conveying a RSA public key?		
Are the KU keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, and decipherOnly bits not set when the NR bit is set in an EE certificate conveying a DSA public key?		
Are the KU keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, and decipherOnly bits not set when the NR bit is set in a CA certificate conveying a DSA public key?		

Other information:

X.509, 11.2 states that a non-repudiation of data service is depends on the archiving of all relevant keys (revoked or expired) and the timestamped revocation lists. The archive must be certified by a current authority.

X.509, B.2 states that non-repudiation security service provides proof of the integrity and origin of data – both in an unforgeable relationship – which can be verified by any third party at any time.

X.509, B.3 states that the non-repudiation service needs the support of both the data integrity and digital signature mechanisms for its requirements to be fully met.

Findings:

Recommendations for Standards Work: